CLAIMS

1. A cyphering/decyphering method, by an integrated circuit, of a digital input code (S_0, S_n) by means of several keys (Ki), consisting of:

dividing said code into several data blocks of same dimensions; and

applying to said blocks several turns (T) of a cyphering or decyphering consisting of submitting each block to at least one same non-linear transformation (SUBBYTES, INVSUBBYTES) and of subsequently combining each block with a different key (Ki) at each turn,

consisting of masking the operands, upon execution of the method, by means of at least one first random number (R1) having the size of said code and all the blocks of which have the same value by combining, by an XOR-type function, the input and output blocks of the non-linear transformation with said random number.

2. The method of claim 1, consisting of combining the input code (S_0, S_n) with a second random number (R) of same dimension as the code.

3. The method of claim 1 , wherein said non-linear transformation (SUBBYTES, INVSUBBYTES) consists of using a box ($SBOX_{R1,R2}$) of substitution of the input code blocks, calculated with a third random number (R2) of same length as said code and all the blocks of which have the same value, said box ($SBOX_{R1,R2}$) respecting the fact that the transformation of an input code, previously combined by XOR with the first random number (R1), corresponds to the result of the combination by XOR of this input code with said third random number.

4. The method of any of claims 1 to 3, applied to an AES-type cyphering algorithm.

5. The method of claim 1, wherein said first random number (R1) is changed at each cyphering turn.

6. The method of claim 2, wherein said second random number (R) is changed at each cyphering of a new datum.

7. The method of claim 3, wherein said third random number (R2) is changed at each cyphering turn.

8. An integrated circuit comprising a block for cyphering/decyphering by turn input data (S_0, S_n) divided into blocks of same dimensions, comprising:

means for generating at least one first random number (R1) of same size as the size of the blocks of the input data; and

means for combining said random number with each block, at the input and at the output of a non-linear transformation (34, 54) implemented by the cyphering/decyphering.

9. The circuit of claim 8, comprising means for implementing the method of any of claims 1 to 7.